PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-368820

(43)Date of publication of application : 20.12.2002

(51)Int.Cl. H04L 12/58
G06F 11/00
G06F 13/00

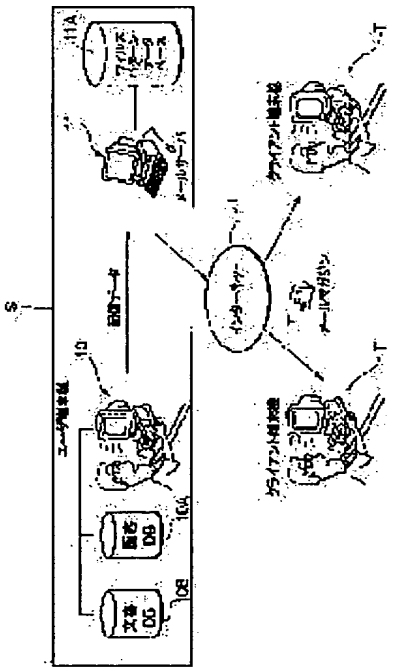
(21)Application number : 2001-172821

(22)Date of filing : 07.06.2001

(71)Applicant : PIONEER ELECTRONIC CORP
INKURIMENTO P KK

(72)Inventor : NOZAKI TAKASHI
NAGANO AKIKO

(54) VIRUS CHECK SYSTEM FOR ELECTRONIC MAIL



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a virus check system that can easily apply virus check to electronic mail such as a mail magazine and quickly distribute electronic mail at a low cost.

SOLUTION: In an electronic mail distribution system distributing electronic mail through a mail server 11, a virus pattern database 11A that records virus pattern data denoting computer virus patterns, and a virus check program that detects presence/absence of virus from electronic mail going to be distributed on the basis of the virus pattern data recorded in the virus pattern database are included.

CLAIMS

[Claim(s)]

[Claim 1]An electronic mail distribution system which distributes an E-mail via a mail server, comprising:

A virus pattern database with which said mail server records virus pattern data in which a pattern of a computer virus is shown.

The Safe Hex program which detects existence of a virus based on virus pattern data currently recorded on a virus pattern database to an E-mail which distributes.

[Claim 2]A virus check system of the E-mail according to claim 1 with which said Safe Hex program includes a virus detection procedure which detects existence of a virus to an attached file of an E-mail.

[Claim 3]A virus extermination procedure of exterminating a virus from the attached file when said Safe Hex program detects a virus being contained in an attached file of an E-mail by said virus detection procedure, A virus check system of the E-mail according to claim 2 include a message insertion procedure which inserts in an E-mail a message of a purport which exterminated a virus.

[Claim 4]When said Safe Hex program detects that a virus is not contained in an attached file of an E-mail by said virus detection procedure, A virus check system of the E-mail according to claim 2 include a message insertion procedure which inserts in an E-mail a message of a purport that it is that a virus ends with an inspection.

[Claim 5]When link information to an offer-of-information site is included in an E-mail, said Safe Hex program, A virus check system of the E-mail according to claim 1 include a virus detection procedure which reads a data file of an offer-of-information site linked by that link information, and detects existence of a virus to this read data file.

[Claim 6]When it detects that a virus is contained in a data file to which said Safe Hex program was read from an offer-of-information site by said virus detection procedure, A virus check system of the E-mail according to claim 5 include a link information deletion procedure of deleting link information to the offer-of-information site from an E-mail.

[Claim 7]When said Safe Hex program deletes link information to an offer-of-information site from an E-mail by said link information deletion procedure, A virus check system of the E-mail according to claim 6 which includes a notification procedure which reports that link information to an offer-of-information site was deleted in a terminal which transmitted the E-mail to a mail server for distribution.

[Claim 8]When it detects that a virus is not contained in a data file to which said Safe Hex program was read from an offer-of-information site by said virus detection procedure, A virus check system of the E-mail according to claim 5 include a message insertion procedure which inserts in an E-mail a message of a purport that it is that a

virus ends with an inspection.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the system for preventing infection of the virus by distribution of an E-mail.

[0002]

[Problem(s) to be Solved by the Invention]Generally, the file for an offer of information is attached to the E-mail distributed for a commuter's ticket or the mail magazine distributed irregularly, the after follow to a customer, etc., or the hyperlink for linking to an FTP site etc. is embedded at it in many cases.

[0003]The addressee of E-mails, such as such a mail magazine, opens the attached file, or, Or when a necessary file is downloaded from the site of a link destination by the hyperlink currently embedded and these files are polluted by the virus. When the addressee's computer system is infected with a virus, there is a possibility that the serious damage of it being downed or important data being destroyed may occur.

[0004]In E-mails, such as a mail magazine especially distributed to a customer from a company, Since what attached the same file or embedded the hyperlink is simultaneously distributed to many clients, If the data file which the attached file is polluted by the virus or is downloaded from a link destination site is polluted by the virus, while the damage will continue broadly and the amount of damage will become large, The situation where trust of the company etc. which distributed E-mails, such as the mail magazine, will fall greatly arises.

[0005]Conventionally, methods, such as carrying out, after entrusting distribution of a mail magazine etc. to the vendor 2 from distribution former 1 and performing Safe Hex, as shown in drawing 3, are taken as preventive measures of such a viral infection.

[0006]However, in such a conventional method, since distribution of a mail magazine etc. is performed via a vendor, the problem that the trouble and time to distribution will be taken or cost will increase has arisen.

[0007]It succeeds in this invention in order to solve the problem at the time of distributing E-mails, such as the above mail magazines.

[0008]That is, this invention can perform Safe Hex easily to E-mails, such as a mail magazine, and an object of the invention is to provide the virus check system which can distribute a quick E-mail by low cost.

[0009]

[Means for Solving the Problem]As for a virus check system of an E-mail by the 1st invention, this invention is characterized by that an electronic mail distribution system which distributes an E-mail via a mail server comprises the following to achieve the above objects.

A virus pattern database with which said mail server records virus pattern data in which a pattern of a computer virus is shown.

The Safe Hex program which detects existence of a virus based on virus pattern data currently recorded on a virus pattern database to an E-mail which distributes.

[0010]A virus check system of an E-mail by this 1st invention, When distribution of an E-mail is performed via a mail server currently installed in the company in a company etc. which distribute E-mails, such as a mail magazine, A virus pattern database with which virus pattern data in which a pattern of a computer virus is shown were recorded on this mail server, Based on virus pattern data currently recorded on this virus pattern database, As opposed to a data file provided by link information to offer-of-information sites, such as an FTP site currently stuck on a file attached to an E-mail which distributes, or an E-mail, It has the Safe Hex program which detects whether a virus is contained or not, and Safe Hex is performed before that distribution in this mail server to an E-mail which distributes.

[0011]And after this Safe Hex performs required processings, such as extermination of a virus, and deletion of link information to an offer-of-information site, to an E-mail with which a virus was detected, for example, that E-mail is distributed.

[0012]As mentioned above, the necessity of according to this 1st invention entrusting distribution of E-mails, such as a mail magazine, to a vendor, and performing it for Safe Hex is lost, and by this. A problem that trouble and time will be taken by distribution or cost will increase can be solved, and a quick E-mail can be distributed now by low cost.

[0013]A virus check system of an E-mail by the 2nd invention, to achieve the above objects, the 1st composition of an invention -- in addition, said Safe Hex program is characterized by including a virus detection procedure which detects existence of a virus to an attached file of an E-mail.

[0014]According to the virus check system of an E-mail by this 2nd invention, Safe Hex by the Safe Hex program is performed by virus detection procedure to an attached file of an E-mail distributed.

[0015]When a virus is contained in an attached file of an E-mail by this, by it, required processing of virus extermination etc. can be performed before distribution of the E-mail in a mail server.

[0016]A virus check system of an E-mail by the 3rd invention, To achieve the above objects, in the 2nd composition of an invention in addition, said Safe Hex program, A virus extermination procedure of exterminating a virus from the attached file when it detects a virus being contained in an attached file of an E-mail by said virus detection procedure, It is characterized by including a message insertion procedure which inserts in an E-mail a message of a purport which exterminated a virus.

[0017]According to the virus check system of an E-mail by this 3rd invention. When it is detected that a virus is contained in an attached file of an E-mail, A virus is exterminated from the attached file by a virus extermination procedure of the Safe Hex program, and after a message of a purport which exterminated a virus to an E-mail by a message insertion procedure is inserted further, distribution of an E-mail is performed.

[0018]While a client which received the E-mail can open an attached file in comfort by this, a viral infection to a client can be prevented beforehand.

[0019]A virus check system of an E-mail by the 4th invention, To achieve the above objects, in the 2nd composition of an invention in addition, when said Safe Hex program detects that a virus is not contained in an attached file of an E-mail by said virus detection procedure, It is characterized by including a message insertion procedure which inserts in an E-mail a message of a purport that it is that a virus ends with an inspection.

[0020]According to the virus check system of an E-mail by this 4th invention. When a message of a purport that the E-mail is that a virus ends with an inspection is inserted in an E-mail distributed by message insertion procedure of the Safe Hex program, A client which received the E-mail can open an attached file now in comfort.

[0021]A virus check system of an E-mail by the 5th invention, To achieve the above objects, in the 1st composition of an invention in addition, when link information to an offer-of-information site is included in an E-mail, said Safe Hex program, It is characterized by reading a data file of an offer-of-information site linked by that link information, and including a virus detection procedure which detects existence of a virus to this read data file.

[0022]According to the virus check system of an E-mail by this 5th invention. Safe Hex by the Safe Hex program is performed to a data file provided by link information to offer-of-information sites, such as an FTP site currently stuck on an E-mail distributed by a virus detection procedure.

[0023]By this, when a data file provided by link information to an offer-of-information site included in an E-mail is polluted by virus, in a mail server, required processing of deletion of the link information, etc. can be performed before distribution of the E-mail.

[0024]A virus check system of an E-mail by the 6th invention, To achieve the above objects, in the 5th composition of an invention in addition, said Safe Hex program, When it detects that a virus is contained in a data file read from an offer-of-information site by said virus detection procedure, it is characterized by including a link information deletion procedure of deleting link information to the offer-of-information site from an E-mail.

[0025]According to the virus check system of an E-mail by this 6th invention. When a data file provided by link information to an offer-of-information site included in an E-mail is polluted by virus, By a link information deletion procedure of the Safe Hex program, the link information is deleted from an E-mail, and distribution of an E-mail is performed after that.

[0026]By this, a viral infection to a client which received the E-mail can be beforehand prevented now.

[0027]A virus check system of an E-mail by the 7th invention, To achieve the above objects, in the 6th composition of an invention in addition, when said Safe Hex program deletes link information to an offer-of-information site from an E-mail by said link information deletion procedure, It is characterized by including a notification procedure which reports that link information to an offer-of-information site was deleted in a terminal which transmitted the E-mail to a mail server for distribution.

[0028]According to the virus check system of an E-mail by this 7th invention. When link information to an offer-of-information site is deleted from an E-mail by detection of a virus, For example, it requested distribution of the E-mail to a mail server, a notice which tells that link information to an offer-of-information site was deleted with a notification procedure of the Safe Hex program is performed to an E-mail distribution person's in charge terminal, etc.

[0029]By this, E-mail distribution persons in charge can know that a data file from an offer-of-information site which it was going to provide was polluted by virus, and that intended offer of information will no longer be performed.

[0030]A virus check system of an E-mail by the 8th invention, To achieve the above objects, in the 5th composition of an invention in addition, said Safe Hex program, When it detects that a virus is not contained in a data file read from an offer-of-information site by said virus detection procedure, it is characterized by including a message insertion procedure which inserts in an E-mail a message of a purport that it is that a virus ends with an inspection.

[0031]According to the virus check system of an E-mail by this 8th invention. When a message of a purport that the E-mail is that a virus ends with an inspection is inserted

in an E-mail distributed by message insertion procedure of the Safe Hex program, A client which received the E-mail can access an offer-of-information site now in comfort based on link information.

[0032]

[Embodiment of the Invention]Hereafter, the embodiment of this invention considered to be the most suitable is described in detail, referring to drawings.

[0033]Drawing 1 is a system configuration figure showing an example of the embodiment of the virus check system of the distribution mail by this invention.

[0034]Although this invention is applicable to the distribution of the E-mail of all gestalten performed via a computer network, such as distribution of an E-mail performed in in the company besides the distribution of a mail magazine performed via the Internet, or distribution of various E-mails, It explains by mentioning as an example the case where distribution of a mail magazine is performed to below from a company etc. to a client.

[0035]In this drawing 1, S shows the distribution system of the mail magazine, It has the customer database 10A by which the customer data which distribute a mail magazine are accumulated in the terminal 10 in which the user who uses this mail magazine distribution system S performs transmit operation of a mail magazine, and the document data base 10B with which the document data of a mail magazine is accumulated.

[0036]And it is connected to the mail server 11 by LAN, the Internet I is accessed via this mail server 11, and this terminal 10 distributes a mail magazine to the client terminal machine T registered into the customer database 10A.

[0037]As for the mail server 11, the Safe Hex program which is mentioned later is stored, It has the virus pattern database 11A with which the virus pattern data used for the collation in the case of Safe Hex by this Safe Hex program are recorded.

[0038]The data which shows the pattern of all the kinds that have become clear of viruses, such as a machine language virus and a macrovirus, to this virus pattern database 11A is stored, and these virus pattern data are updated as required, whenever a new type of virus is discovered.

[0039]When distribution of a mail magazine is performed by mail magazine distribution system S, the mail magazine which distributes is created based on the operational input by the mail delivery person in charge to the terminal 10.

[0040]Although creation of a mail magazine is performed by the method of searching required data out of the document data accumulated in the document data base 10B at this time, and constituting the read document data, At this time, the file for attachment

to the mail magazine is beforehand registered into the document data base 10B, or, It is registered by the link information to the FTP site which an HTML file, online software, etc. have uploaded, and a mail delivery person in charge, The mail magazine to distribute is created by reading the required file for attachment from this document data base 10B, attaching, or reading the link information to an FTP site and sticking a hyperlink.

[0041]And next, the client which distributes a mail magazine out of the customer registered into the customer database 10A is searched, and the address data of the client are read from the customer database 10A.

[0042]Thus, if preparation of distribution of a mail magazine is completed, a mail delivery person in charge will transmit the distributes data of the mail magazine to the mail server 11.

[0043]Before the mail server 11 which received the distributes data of this mail magazine performs distribution of that mail magazine, it starts the Safe Hex program stored in this mail server 11, and performs Safe Hex to that distributes data.

[0044]Drawing 2 is a flow chart which shows the procedure of Safe Hex performed by the Safe Hex program in this mail server 11.

[0045]Next, the procedure of Safe Hex is explained based on this drawing 2.

[0046]First, the mail server 11 judges whether the data of the attached file is contained in the distributes data, when it judges whether the distributes data of a mail magazine has been transmitted from the terminal 10 (Step S1) and distributes data has been transmitted next (Step S2).

[0047]When it is judged in this step S2 that the data of an attached file is contained in the distributes data of a mail magazine, The data of the attached file is compared with all the virus pattern data read from the virus pattern database 11A (Step S3), It is detected whether the program which has a pattern which is the same as virus pattern data, or is approximated is included in the data of the attached file (step S4).

[0048]If it is detected that the program which has a pattern which is the same as virus pattern data to the data of an attached file, or is approximated to it in this step S4 is included, A computer virus is exterminated with the vaccine software with which the Safe Hex program is provided (Step S5).

[0049]And in Step S5, when a computer virus is exterminated, the data for displaying the message of a purport "which exterminated the computer virus to the attached file" in the distributes data of a mail magazine is inserted (Step S6).

[0050]When the program which has a pattern which is the same as virus pattern data, or is approximated is not detected from the data of an attached file in step S4, The data

for displaying the message of the purport "an attached file is Safe Hex ending" in the distributes data of a mail magazine is inserted (step S6').

[0051]Next, it is detected whether the hyperlink to the FTP site is contained in the distributes data of a mail magazine (Step S7).

[0052]When it is detected in this step S7 that the hyperlink to an FTP site is contained in the distributes data of a mail magazine, Based on the hyperlink, the linked upload data of a necessary HTML file, online software, etc. is read from an FTP site (Step S8), Safe Hex is performed by the same method as the above-mentioned step S4 to this HTML file, online software, etc. that were read (step S9).

[0053]If it is detected that the program which has a pattern which is the same as virus pattern data to an HTML file, online software, etc. which were read from the FTP site, or is approximated to them in this step S9 is included, The hyperlink from distributes data to this FTP site is deleted (Step S10).

[0054]And in Step S10, when the hyperlink to an FTP site is deleted, the E-mail which notifies the distribution person in charge of a mail magazine of "the hyperlink was deleted" is replied to the distribution person's in charge terminal 10 (Step S11).

[0055]When the program which has a pattern which is the same as virus pattern data, or is approximated is detected from neither the HTML file read from the FTP site, nor online software in step S9, The data for displaying the message of the purport "the FTP site of a link destination is Safe Hex ending" in the distributes data of a mail magazine is inserted (step S11').

[0056]The mail server 11 performs distribution of a mail magazine to each client terminal machine T after Safe Hex to the above distributes data based on distributes data [finishing / the Safe Hex] (Step S12).

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a system configuration figure showing an example of the embodiment of this invention.

[Drawing 2]It is a flow chart which shows the procedure of Safe Hex in the example.

[Drawing 3]It is an explanatory view showing a conventional example.

[Description of Notations]

10 -- Terminal

10A -- Customer database

10B -- Document data base

11 -- Mail server

11A -- Virus pattern database

S -- Mail magazine distribution system

I -- the Internet

T -- Client terminal machine

---

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－368820
（P2002－368820A）
(43)公開日　平成14年12月20日(2002.12.20)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
H04L 12/58	100	H04L 12/58	100F 5B076
G06F 11/00		G06F 13/00	610Q 5K030
13/00	610	9/06	660N

審査請求　未請求　請求項の数８　ＯＬ　（全 7 頁）

(21)出願番号　特願2001－172821(P2001－172821)

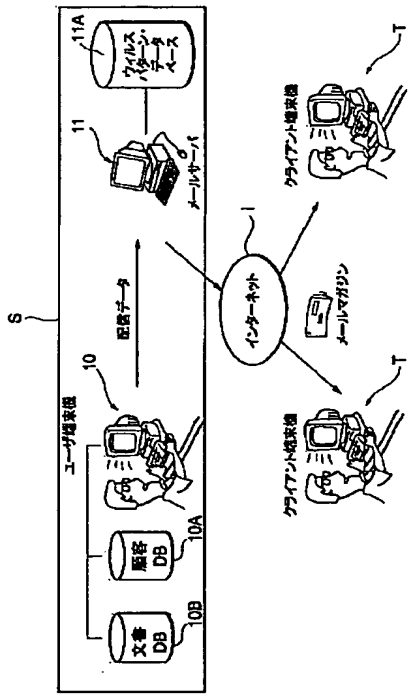
(22)出願日　平成13年６月７日(2001.6.7)

(71)出願人　000005016
パイオニア株式会社
東京都目黒区目黒１丁目４番１号
(71)出願人　595105515
インクリメント・ピー株式会社
東京都目黒区下目黒１丁目７番１号
(72)発明者　野崎　隆志
東京都目黒区下目黒１丁目７番１号ＰＡＸビル１階　インクリメント・ピー株式会社内
(74)代理人　100063565
弁理士　小橋　信淳　（外１名）

最終頁に続く

(54)【発明の名称】　電子メールのウィルスチェックシステム

(57)【要約】
【課題】　メールマガジン等の電子メールに対して容易にウィルスチェックを行うことができ、低コストで迅速な電子メールの配信を行うことができるウィルスチェックシステムを提供する。
【解決手段】　メールサーバ１１を介して電子メールを配信する電子メール配信システムにおいて、メールサーバ１１が、コンピュータウィルスのパターンを示すウィルスパターン・データを記録するウィルスパターン・データベース１１Ａと、配信を行う電子メールに対してウィルスパターン・データベースに記録されているウィルスパターン・データに基づいてウィルスの有無の検出を行うウィルスチェック・プログラムとを備えている。



【特許請求の範囲】

【請求項１】　メールサーバを介して電子メールを配信する電子メール配信システムにおいて、
前記メールサーバが、コンピュータウィルスのパターンを示すウィルスパターン・データを記録するウィルスパターン・データベースと、配信を行う電子メールに対してウィルスパターン・データベースに記録されているウィルスパターン・データに基づいてウィルスの有無の検出を行うウィルスチェック・プログラムとを備えていることを特徴とする電子メールのウィルスチェックシステム。

【請求項２】　前記ウィルスチェック・プログラムが、電子メールの添付ファイルに対してウィルスの有無の検出を行うウィルス検出手順を含んでいる請求項１に記載の電子メールのウィルスチェックシステム。

【請求項３】　前記ウィルスチェック・プログラムが、前記ウィルス検出手順によって電子メールの添付ファイルにウィルスが含まれていることを検出したときにその添付ファイルからウィルスを駆除するウィルス駆除手順と、電子メールにウィルスを駆除した旨のメッセージを挿入するメッセージ挿入手順を含んでいる請求項２に記載の電子メールのウィルスチェックシステム。

【請求項４】　前記ウィルスチェック・プログラムが、前記ウィルス検出手順によって電子メールの添付ファイルにウィルスが含まれていないことを検出したときに、電子メールにウィルスの検査済みである旨のメッセージを挿入するメッセージ挿入手順を含んでいる請求項２に記載の電子メールのウィルスチェックシステム。

【請求項５】　前記ウィルスチェック・プログラムが、電子メールに情報提供サイトへのリンク情報が含まれているときに、そのリンク情報によってリンクされる情報提供サイトのデータファイルを読み出して、この読み出されたデータファイルに対してウィルスの有無の検出を行うウィルス検出手順を含んでいる請求項１に記載の電子メールのウィルスチェックシステム。

【請求項６】　前記ウィルスチェック・プログラムが、前記ウィルス検出手順によって情報提供サイトから読み出されたデータファイルにウィルスが含まれていることを検出したときに、その情報提供サイトへのリンク情報を電子メールから削除するリンク情報削除手順を含んでいる請求項５に記載の電子メールのウィルスチェックシステム。

【請求項７】　前記ウィルスチェック・プログラムが、前記リンク情報削除手順によって情報提供サイトへのリンク情報を電子メールから削除したときに、その電子メールを配信のためにメールサーバに送信した端末機に情報提供サイトへのリンク情報を削除した旨の通知を行う通知手順を含んでいる請求項６に記載の電子メールのウィルスチェックシステム。

【請求項８】　前記ウィルスチェック・プログラムが、

前記ウィルス検出手順によって情報提供サイトから読み出されたデータファイルにウィルスが含まれていないことを検出したときに、電子メールにウィルスの検査済みである旨のメッセージを挿入するメッセージ挿入手順を含んでいる請求項５に記載の電子メールのウィルスチェックシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電子メールの配信によるウィルスの感染を防止するためのシステムに関する。

【０００２】

【発明が解決しようとする課題】一般に、定期または不定期に配信されるメールマガジンや顧客へのアフタフォローなどのために配信される電子メールなどには、情報提供のためのファイルが添付されていたり、ＦＴＰサイトなどにリンクするためのハイパーリンクが埋め込まれていたりすることが多い。

【０００３】このようなメールマガジン等の電子メールの受信者が、その添付ファイルを開いたり、または、埋め込まれているハイパーリンクによってリンク先のサイトから所要のファイルをダウンロードした際に、これらのファイルがウィルスに汚染されていた場合には、その受信者のコンピュータシステムがウィルスに感染することによって、ダウンしてしまったり、大事なデータが破壊されてしまったりするなどの重大な被害が発生する虞がある。

【０００４】特に、企業から顧客に配信されるメールマガジンなどの電子メールにおいては、同じファイルを添付したりハイパーリンクを埋め込んだりしたものが同時に多数のクライアントに対して配信されるために、添付ファイルがウィルスに汚染されていたりリンク先サイトからダウンロードされるデータファイルがウィルスに汚染されていると、その被害は広範囲に亘ってしまい、その損害額が大きくなるとともに、そのメールマガジン等の電子メールを配信した企業などの信用が大きく低下してしまうといった事態が生じる。

【０００５】従来、このようなウィルス感染の防止対策として、図３に示されるように、メールマガジン等の配信を、その配信元１から専門業者２に委託してウィルスチェックを行った後に行うなどの方法が採られている。

【０００６】しかしながら、このような従来の方法では、メールマガジン等の配信が専門業者を介して行われるために、配信までの手数や時間がかかったり、コストが嵩んでしまうといった問題が生じている。

【０００７】この発明は、上記のようなメールマガジン等の電子メールを配信する際の問題点を解決するために為されたものである。

【０００８】すなわち、この発明は、メールマガジン等の電子メールに対して容易にウィルスチェックを行うこ

とができ、低コストで迅速な電子メールの配信を行うことができるウィルスチェックシステムを提供することを目的としている。

【０００９】

【課題を解決するための手段】第１の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、メールサーバを介して電子メールを配信する電子メール配信システムにおいて、前記メールサーバが、コンピュータウィルスのパターンを示すウィルスパターン・データを記録するウィルスパターン・データベースと、配信を行う電子メールに対してウィルスパターン・データベースに記録されているウィルスパターン・データに基づいてウィルスの有無の検出を行うウィルスチェック・プログラムとを備えていることを特徴としている。

【００１０】この第１の発明による電子メールのウィルスチェックシステムは、メールマガジンなどの電子メールの配信を行う企業等において、電子メールの配信がその企業等に設置されているメールサーバを介して行われる場合に、このメールサーバに、コンピュータウィルスのパターンを示すウィルスパターン・データが記録されたウィルスパターン・データベースと、このウィルスパターン・データベースに記録されているウィルスパターン・データに基づいて、配信を行う電子メールに添付されているファイルや電子メールに貼り付けられているＦＴＰサイト等の情報提供サイトへのリンク情報によって提供されるデータファイルに対して、ウィルスが含まれているか否かの検出を行うウィルスチェック・プログラムを備えて、このメールサーバにおいて、配信を行う電子メールに対してその配信前に、ウィルスチェックを行う。

【００１１】そして、このウィルスチェックによってウィルスが検出された電子メールに対しては、例えば、ウイルスの駆除や情報提供サイトへのリンク情報の削除といった必要な処理を行った後に、その電子メールの配信を行う。

【００１２】以上のように、この第１の発明によれば、メールマガジン等の電子メールの配信を、ウィルスチェックのために専門業者に委託して行う必要が無くなり、これによって、配信までに手数や時間がかかったりコストが嵩んでしまうといった問題が解消出来、低コストで迅速な電子メールの配信を行うことができるようになる。

【００１３】第２の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、第１の発明の構成に加えて、前記ウィルスチェック・プログラムが、電子メールの添付ファイルに対してウィルスの有無の検出を行うウィルス検出手順を含んでいることを特徴としている。

【００１４】この第２の発明による電子メールのウィルスチェックシステムによれば、ウィルスチェック・プログラムによるウィルスチェックが、ウィルス検出手順によって、配信される電子メールの添付ファイルに対して行われる。

【００１５】これによって、電子メールの添付ファイルにウィルスが含まれている場合には、メールサーバにおいてその電子メールの配信前に、ウィルス駆除等の必要な処理を行うことが出来るようになる。

【００１６】第３の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、第２の発明の構成に加えて、前記ウィルスチェック・プログラムが、前記ウィルス検出手順によって電子メールの添付ファイルにウィルスが含まれていることを検出したときにその添付ファイルからウィルスを駆除するウィルス駆除手順と、電子メールにウィルスを駆除した旨のメッセージを挿入するメッセージ挿入手順を含んでいることを特徴としている。

【００１７】この第３の発明による電子メールのウィルスチェックシステムによれば、電子メールの添付ファイルにウィルスが含まれていることが検出されたときに、ウィルスチェック・プログラムのウィルス駆除手順によってその添付ファイルからウィルスが駆除され、さらに、メッセージ挿入手順によって電子メールにウィルスを駆除した旨のメッセージが挿入された後に、電子メールの配信が実行される。

【００１８】これによって、その電子メールを受信したクライアントが安心して添付ファイルを開くことが出来るとともに、クライアントへのウィルス感染を未然に防止することが出来るようになる。

【００１９】第４の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、第２の発明の構成に加えて、前記ウィルスチェック・プログラムが、前記ウィルス検出手順によって電子メールの添付ファイルにウィルスが含まれていないことを検出したときに、電子メールにウィルスの検査済みである旨のメッセージを挿入するメッセージ挿入手順を含んでいることを特徴としている。

【００２０】この第４の発明による電子メールのウィルスチェックシステムによれば、ウィルスチェック・プログラムのメッセージ挿入手順によって、配信される電子メールに、その電子メールがウィルスの検査済みである旨のメッセージが挿入されることによって、その電子メールを受信したクライアントが安心して添付ファイルを開くことが出来るようになる。

【００２１】第５の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、第１の発明の構成に加えて、前記ウィルスチェック・プログラムが、電子メールに情報提供サイトへのリンク情報が含まれているときに、そのリンク情報によってリンクされる情報提供サイトのデータファイルを読み出して、この

読み出されたデータファイルに対してウィルスの有無の検出を行うウィルス検出手順を含んでいることを特徴としている。

【００２２】この第５の発明による電子メールのウィルスチェックシステムによれば、ウィルスチェック・プログラムによるウィルスチェックが、ウィルス検出手順によって、配信される電子メールに貼り付けられているＦＴＰサイト等の情報提供サイトへのリンク情報によって提供されるデータファイルに対して行われる。

【００２３】これによって、電子メールに含まれる情報提供サイトへのリンク情報によって提供されるデータファイルがウィルスに汚染されている場合には、メールサーバにおいてその電子メールの配信前に、そのリンク情報の削除等の必要な処理を行うことが出来るようになる。

【００２４】第６の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、第５の発明の構成に加えて、前記ウィルスチェック・プログラムが、前記ウィルス検出手順によって情報提供サイトから読み出されたデータファイルにウィルスが含まれていることを検出したときに、その情報提供サイトへのリンク情報を電子メールから削除するリンク情報削除手順を含んでいることを特徴としている。

【００２５】この第６の発明による電子メールのウィルスチェックシステムによれば、電子メールに含まれる情報提供サイトへのリンク情報によって提供されるデータファイルがウィルスに汚染されている場合には、ウィルスチェック・プログラムのリンク情報削除手順によってそのリンク情報が電子メールから削除され、その後に、電子メールの配信が実行される。

【００２６】これによって、その電子メールを受信したクライアントへのウィルス感染を未然に防止することが出来るようになる。

【００２７】第７の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、第６の発明の構成に加えて、前記ウィルスチェック・プログラムが、前記リンク情報削除手順によって情報提供サイトへのリンク情報を電子メールから削除したときに、その電子メールを配信のためにメールサーバに送信した端末機に情報提供サイトへのリンク情報を削除した旨の通知を行う通知手順を含んでいることを特徴としている。

【００２８】この第７の発明による電子メールのウィルスチェックシステムによれば、情報提供サイトへのリンク情報がウィルスの検出によって電子メールから削除された際に、その電子メールの配信をメールサーバに対して依頼した例えば電子メール配信担当者の端末機などに、ウィルスチェック・プログラムの通知手順によって、情報提供サイトへのリンク情報が削除されたことを知らせる通知が行われる。

【００２９】これによって、電子メール配信担当者等は、提供しようとした情報提供サイトからのデータファイルがウィルスに汚染されていたこと、および、意図した情報の提供が行われなくなったことを知ることが出来る。

【００３０】第８の発明による電子メールのウィルスチェックシステムは、上記目的を達成するために、第５の発明の構成に加えて、前記ウィルスチェック・プログラムが、前記ウィルス検出手順によって情報提供サイトから読み出されたデータファイルにウィルスが含まれていないことを検出したときに、電子メールにウィルスの検査済みである旨のメッセージを挿入するメッセージ挿入手順を含んでいることを特徴としている。

【００３１】この第８の発明による電子メールのウィルスチェックシステムによれば、ウィルスチェック・プログラムのメッセージ挿入手順によって、配信される電子メールに、その電子メールがウィルスの検査済みである旨のメッセージが挿入されることによって、その電子メールを受信したクライアントがリンク情報に基づいて、安心して情報提供サイトにアクセスすることが出来るようになる。

【００３２】

【発明の実施の形態】以下、この発明の最も好適と思われる実施の形態について、図面を参照しながら詳細に説明を行う。

【００３３】図１は、この発明による配信メールのウィルスチェックシステムの実施形態の一例を示すシステム構成図である。

【００３４】なお、この発明は、インターネットを介して行われるメールマガジンの配信や各種電子メールの配信の他、社内において行われる電子メールの配信など、コンピュータ・ネットワークを介して行われるあらゆる形態の電子メールの配信について適用が可能であるが、以下においては、クライアントに対して企業などからメールマガジンの配信が行われる場合を例に挙げて説明を行う。

【００３５】この図１において、Ｓはメールマガジンの配信システムを示しており、このメールマガジン配信システムＳを使用するユーザがメールマガジンの送信操作を行う端末機１０に、メールマガジンの配信を行う顧客情報が蓄積される顧客データベース１０Ａと、メールマガジンの文書データが蓄積される文書データベース１０Ｂが備えられている。

【００３６】そして、この端末機１０は、ＬＡＮによってメールサーバ１１に接続され、このメールサーバ１１を介してインターネットＩに接続されて、顧客データベース１０Ａに登録されているクライアント端末機Ｔにメールマガジンの配信を行うようになっている。

【００３７】メールサーバ１１は、その後述するようなウィルスチェック・プログラムが格納されており、さらに、このウィルスチェック・プログラムによるウィルス

チェックの際の照合に使用されるウィルスパターン・データが記録されるウィルスパターン・データベース１１Ａを備えている。

【００３８】このウィルスパターン・データベース１１Ａには、機械語ウィルスおよびマクロウィルス等、判明しているあらゆる種類のウィルスのパターンを示すデータが蓄積され、このウィルスパターン・データは、新種のウィルスが発見されるごとに、随時、更新される。

【００３９】メールマガジン配信システムＳによってメールマガジンの配信が行われる際には、端末機１０へのメール配信担当者による操作入力に基づいて、配信を行うメールマガジンが作成される。

【００４０】このとき、文書データベース１０Ｂに蓄積されている文書データの中から必要なデータを検索して、読み出された文書データを構成する等の方法によりメールマガジンの作成が行われるが、このとき、文書データベース１０Ｂには、メールマガジンへの添付用ファイルがあらかじめ登録されていたり、ＨＴＭＬファイルやオンラインソフトなどがアップロードされているＦＴＰサイトへのリンク情報が登録されていて、メール配信担当者は、この文書データベース１０Ｂから必要な添付用ファイルを読み出して添付したり、ＦＴＰサイトへのリンク情報を読み出してハイパーリンクを貼り付けたりすることによって、配信するメールマガジンの作成を行ってゆく。

【００４１】そして、次に、顧客データベース１０Ａに登録されている顧客のなかからメールマガジンの配信を行うクライアントの検索を行って、そのクライアントのアドレス・データを顧客データベース１０Ａから読み出す。

【００４２】このようにして、メールマガジンの配信の準備が完了すると、メール配信担当者は、そのメールマガジンの配信データをメールサーバ１１に送信する。

【００４３】このメールマガジンの配信データを受信したメールサーバ１１は、そのメールマガジンの配信を実行する前に、このメールサーバ１１に格納されているウィルスチェック・プログラムを起動して、その配信データに対するウィルスチェックを行う。

【００４４】図２は、このメールサーバ１１においてウィルスチェック・プログラムにより行われるウィルスチェックの手順を示すフローチャートである。

【００４５】次に、この図２に基づいて、ウィルスチェックの手順について説明を行う。

【００４６】先ず、メールサーバ１１は、端末機１０からメールマガジンの配信データが送信されてきたか否かの判断を行って（ステップＳ１）、配信データが送信されてきたときには、次に、その配信データに添付ファイルのデータが含まれているか否かの判断を行う（ステップＳ２）。

【００４７】このステップＳ２において、メールマガジンの配信データに添付ファイルのデータが含まれていると判断される場合には、その添付ファイルのデータを、ウィルスパターン・データベース１１Ａから読み出される全てのウィルスパターン・データと照合し（ステップＳ３）、ウィルスパターン・データと同一または近似するパターンを有するプログラムが添付ファイルのデータに含まれているか否かの検出を行う（ステップＳ４）。

【００４８】このステップＳ４において、添付ファイルのデータにウィルスパターン・データと同一または近似するパターンを有するプログラムが含まれていることが検出されると、ウィルスチェック・プログラムが備えているワクチンソフトウェアによって、コンピュータウィルスを駆除する（ステップＳ５）。

【００４９】そして、ステップＳ５において、コンピュータウィルスの駆除を行ったときには、メールマガジンの配信データ内に、「添付ファイルに対してコンピュータウィルスの駆除を行った」旨のメッセージを表示するためのデータを挿入する（ステップＳ６）。

【００５０】また、ステップＳ４において、添付ファイルのデータからウィルスパターン・データと同一または近似するパターンを有するプログラムが検出されない場合には、メールマガジンの配信データ内に、「添付ファイルはウィルスチェック済みである」旨のメッセージを表示するためのデータを挿入する（ステップＳ６’）。

【００５１】次に、メールマガジンの配信データに、ＦＴＰサイトへのハイパーリンクが含まれているか否かの検出を行う（ステップＳ７）。

【００５２】このステップＳ７において、メールマガジンの配信データにＦＴＰサイトへのハイパーリンクが含まれていることが検出されたときには、そのハイパーリンクに基づいて、ＦＴＰサイトから、リンクしている所要のＨＴＭＬファイルやオンラインソフトなどのアップロードデータの読み出しを行い（ステップＳ８）、この読み出されたＨＴＭＬファイルやオンラインソフトなどに対して、上記のステップＳ４と同様の方法により、ウィルスチェックを行う（ステップＳ９）。

【００５３】このステップＳ９において、ＦＴＰサイトから読み出されたＨＴＭＬファイルやオンラインソフトなどにウィルスパターン・データと同一または近似するパターンを有するプログラムが含まれていることが検出されると、配信データから、このＦＴＰサイトへのハイパーリンクを削除する（ステップＳ１０）。

【００５４】そして、ステップＳ１０において、ＦＴＰサイトへのハイパーリンクを削除したときには、「ハイパーリンクの削除を行った」旨をメールマガジンの配信担当者に通知する電子メールを、その配信担当者の端末機１０に返信する（ステップＳ１１）。

【００５５】また、ステップＳ９において、ＦＴＰサイトから読み出されたＨＴＭＬファイルやオンラインソフトなどからウィルスパターン・データと同一または近似

するパターンを有するプログラムが検出されない場合には、メールマガジンの配信データ内に、「リンク先のＦＴＰサイトはウィルスチェック済みである」旨のメッセージを表示するためのデータを挿入する（ステップＳ１１'）。

【００５６】以上のような配信データに対するウィルスチェックの後、メールサーバ１１は、そのウィルスチェック済みの配信データに基づいて、各クライアント端末機Ｔに対して、メールマガジンの配信を実行する（ステップＳ１２）。

【図面の簡単な説明】

【図１】この発明の実施形態の一例を示すシステム構成図である。

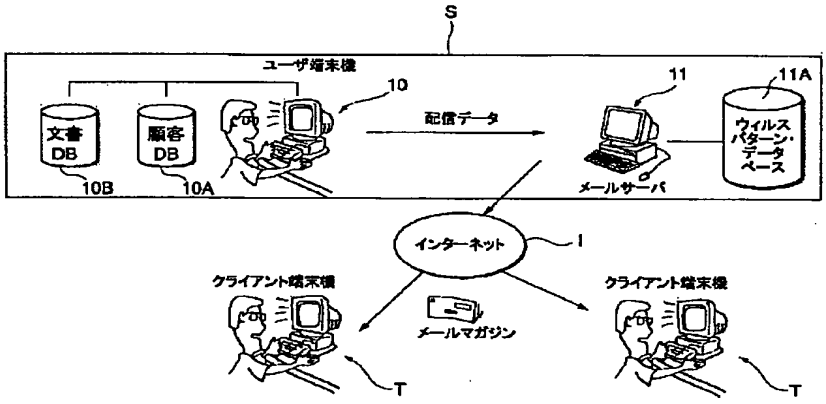
＊【図２】同例におけるウィルスチェックの手順を示すフローチャートである。

【図３】従来例を示す説明図である。

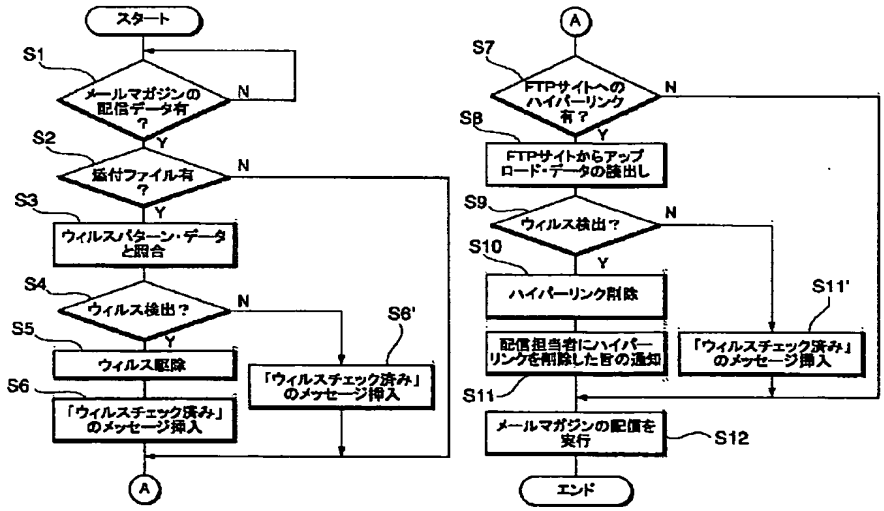
【符号の説明】

１０	…端末機
１０Ａ	…顧客データベース
１０Ｂ	…文書データベース
１１	…メールサーバ
１１Ａ	…ウィルスパターン・データベース
Ｓ	…メールマガジン配信システム
Ｉ	…インターネット
Ｔ	…クライアント端末機

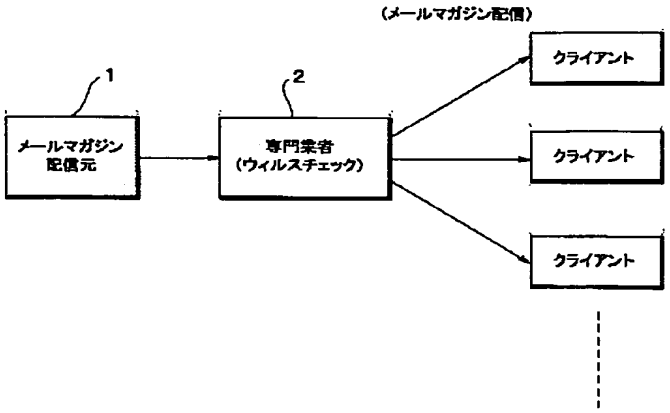
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　永野　明子
東京都目黒区下目黒１丁目７番１号ＰＡＸビル１階　インクリメント・ピー株式会社内

Ｆターム(参考)　5B076 FD08
5K030 GA15 HA06 KA01 KA06 KA07
LC18 LD17 LE12